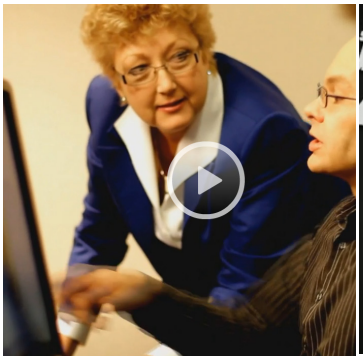
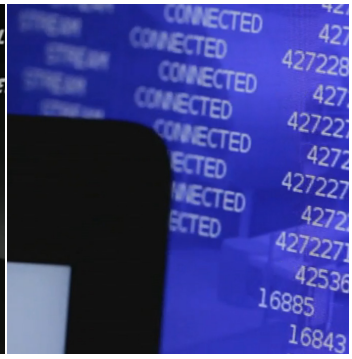
Michigan Cybersecurity Initiatives Reduce Risks Through Improved Employee Training





EXECUTIVE SUMMARY

Objectives

- Reduce security risks through better-trained employees and residents
- Coordinate with private sector regarding critical infrastructure and cybersecurity
- Create opportunities for ongoing education and security

Strategy

- Coordinate with Michigan State Police and other governmental parties responsible for statewide emergency management

Solutions

- Online and group training of state employees
- Cyber Range allows technological staff to practice data security exercises
- Cyber Disruption Strategy formed in collaboration with both public and private entities to address possibility of large-scale cyber attack

Impact

- Garnered "A" grade in 2012 NASCIO Digital States Awards, one of only two states so honored
- Better-trained employees and residents; reduced security risks
- More than a dozen serious cyber threats avoided; decreased damage due to malware and phishing scams
- Estimated program ROI: more than 100:1
- New opportunities for ongoing education and security

Background

In January 2014, Cisco released the results of an in-depth analysis of the economic benefits of the Internet of Everything (IoE) for the public sector. Cisco's model revealed that some $4.6 trillion in "Value at Stake" would result from the adoption of IoE capabilities across 40 key public sector use cases over the next 10 years, including smart water, smart buildings, smart energy, smart parking, and more (http://bit.ly/1aSGlzn).

As a next phase of its analysis, Cisco engaged Cicero Group, a leading data-driven strategy consulting and research firm, to undertake a global study of IoE capabilities across these 40 use cases – how the best public sector organizations are "connecting the unconnected," as Cisco terms it. To that end, Cicero Group conducted interviews with dozens of leading public sector jurisdictions – federal, state, and local governments; healthcare organizations; educational institutions; and non-governmental organizations (NGOs) – to explore how these global leaders are leveraging IoE today.

The research examined real-world projects that are operational today, are being delivered at scale (or through pilots with obvious potential to scale), and that represent the cutting edge of public sector IoE readiness and maturity. The aim of the research was to understand what has changed in terms of the jurisdictions' people, processes, data, and things, and how other public sector organizations can learn from (and replicate) the trail blazed by these global IoE leaders. In many cases, these jurisdictions are Cisco customers; in others, they are not. The focus of these jurisdictional profiles, therefore, is not to tout Cisco's role in these organizations' success, but rather to document IoE excellence, how public sector entities are putting IoE into practice today, and to inform a roadmap for change that will enable the public sector to address pressing challenges on multiple fronts by drawing on best practices from around the globe.

About the State of Michigan

The State of Michigan has implemented a series of cybersecurity initiatives that place it among the top U.S. states for data security awareness and education. These initiatives include an innovative and entertaining employee training program, a Cyber Range where technical specialists learn to counter security threats, and regular public/private collaboration in the creation of the Michigan Cyber Disruption Response Strategy.

Dan Lohrmann serves as chief security officer, chief information security officer, and deputy director of cybersecurity and infrastructure protection (CIP) within the Michigan Department of Technology, Management and Budget (DTMB). Mr. Lohrmann has worked in a variety of public sector security and leadership capacities, including work for the National Security Admininistration (NSA). He was chief information security officer (CISO) and chief technology officer (CTO) for Michigan before assuming his current position.

The State of Michigan has implemented a series of cybersecurity initiatives that place it among the top U.S. states for data security awareness and education.

Andris Ozols is a senior policy adviser and analyst for the State of Michigan Department of Information Technology. He has more than 42 years of experience as a Michigan public employee.

Objectives

The primary objective of Michigan's cybersecurity initiatives was to reduce security risks through better-trained employees and residents. The state also sought to coordinate with the private sector regarding critical infrastructure and cybersecurity, and to create opportunities for ongoing education and security.

Strategy

The State of Michigan chief security officer and the Michigan Department of Technology, Management and Budget are responsible for the overall administration and maintenance of the state's cybersecurity initiative plan and implementation. These efforts are coordinated with the Michigan State Police and other governmental parties responsible for statewide emergency management.

Most funding for Michigan cybersecurity initiatives is public, using a variety of both state and federal sources. This includes grants from the Department of Homeland Security and resources available through collaboration with higher education entities.

- Cyber Summits and Breakfast Conference events are self-supporting through sponsorships and fees for attendance.
- The Security Mentor online training program was established for under $200,000, estimated at a per-employee cost of about 30 cents per lesson over a two-year period.
- The Michigan Cyber Range was created with the assistance of $2 million in private donations and grants, with an additional 20 percent of total funding provided by government sources. It is expected that the state government is saving 40 to 50 percent in certification, course, and travel costs through use of the program.

Solution

As Michigan's chief security officer, and in cooperation with Michigan Governor Rick Snyder, Mr. Lohrmann oversees the state's cybersecurity program, The Michigan Cyber Initiative. Components include online and group training of state employees; a "Cyber Range" setting that allows technological staff to practice data security exercises; and a Cyber Disruption Strategy formed in collaboration with both public and private entities – such as large employers, utilities, and federal agencies – to address the possibility of a large-scale cyber attack.

Employee and Public Training

The state's bimonthly online cybersecurity training program is the core of its employee training system. Mr. Lohrmann's organization also holds Security Summits and a Breakfast Conference Series, and publishes a monthly newsletter.

In beginning the online training program, Mr. Lohrmann first surveyed employees to determine the effectiveness of the existing program, which consisted largely of emailing messages containing hyperlinks to security information videos. The results weren't encouraging.

"We went from about 10 percent of state employees actually taking the training in the last 12 months to well over 90 percent. We were delighted with the number of people who went through the training."

Dan Lohrmann,

Chief Security Officer, Chief Information Security Officer, and Deputy Director of Cybersecurity and Infrastructure Protection,

Michigan Department of Technology, Management and Budget

Mr. Lohrmann recalled, "In some test studies, people were starting the videos, then going down the hall, getting a cup of coffee, heading to the restroom, coming back, talking about the game last night, and hanging out. They weren't even watching the videos. That was not good. We wanted it be interactive. We wanted people to really engage with the training, and most of all, we wanted it to change behavior. It wasn't just about checking the box and saying, 'Yes, I took the cybersecurity training.'"

To find a better way to engage state employees, Mr. Lohrmann followed up with a second survey. "We put together a team to determine what people wanted in the training. People said they wanted it to be timely. They didn't want a two-hour or even an hour-long training at their desk. People wanted it to be brief but frequent. They wanted it to be updated regularly. They wanted it to be intriguing. They wanted it to be fun."

Mr. Lohrmann said DTMB issued a Request for Proposal (RFP) for a more interactive training experience, challenging vendors with the question: "How can we actually change behaviors and have metrics around that?"

DTMB selected a vendor program that used games and interactive activities focused on promoting safe behaviors in a variety of settings. The program was rolled out to all state employees over six months with an outstanding response and positive feedback. "We went from about 10 percent of state employees actually taking the training in the last 12 months to well over 90 percent. We were delighted with the number of people who went through the training."

"Most astounding was that the feedback was just fantastic," Mr. Lohrmann continued. "People said, 'We love this, it's the best thing to ever come out of the technology department,' and we got really wild comments like, 'This is incredible, can I bring it home? Can I show it to my family? Can I use it with my kids?' After every lesson ... they give a grade from one to five, with five being awesome, one

being they didn't like it. With 50,000 state employees, we're averaging over four, which is unheard of in this space."

Mr. Lohrmann explained the appeal of typical training exercises: "One of the games that I liked the best covers the importance of your role in your office, which teaches employees to find security violations such as leaving confidential papers on desks. Then you classify why something was a policy violation or a security violation." Another game involves a Super Mario type of character who runs around an airport looking for 12 lost or stolen laptops. "It's like a countdown – you have 90 seconds," Mr. Lohrmann explained. "The first time I played it, I think I found seven of the 12."

Mr. Lohrmann said the most important aspect of the training is its highly memorable nature. "The idea is to change behaviors; when I go into airports now, I actually can't stop thinking about that Super Mario game," he said. "Whether you're at the ticket counter or the security gate, you think about this stuff. Employees just love it. People say they look forward to taking the lessons."

"The goal was to make it a public-private partnership – to bring in universities and our federal partners to help determine how we prepare to defend our networks and systems against the best and brightest in the world."

Dan Lohrmann,

Chief Security Officer, Chief Information Security Officer, and Deputy Director of Cybersecurity and Infrastructure Protection,

Michigan Department of Technology, Management and Budget

Michigan Cyber Range

In an effort to provide more technical training to IT staff, Mr. Lohrmann sought to re-create a cybersecurity testing environment similar to the ones used during his tenure with the NSA. "The idea was to set up an organization and a training, which we call the Michigan Cyber Range," he explained. "The Cyber Range provides a place to test and train and learn and grow in an unclassified environment. The goal was make it a public-private partnership – to bring in universities and our federal partners to help determine how we prepare to defend our networks and systems against the best and brightest in the world."

According to Mr. Lohrmann, the Cyber Range provides technical training covering topics such as ethical hacking and different types of forensics at about half the cost of sending someone out of state to attend a similar training.

Mr. Ozols also emphasized the broad approach in planning, saying, "We consciously and deliberately take a statewide perspective working with local governments and entities. It is equally a part of our responsibility and in our vision and goals." Cybersecurity experts throughout the state and around the Midwest now use the site regularly, including the National Guard.

Mr. Lohrmann said that he first took his idea for a cyber skills test site to Governor Snyder, who strongly backed the project. Mr. Lohrmann then recruited a software firm to develop the test platform – an unclassified, logically isolated system that allows technical teams to learn data security techniques through a series of exercises.

Mr. Lohrmann's technical teams practice skills with a variety of tabletop scenarios, including "Alphaville," which Mr. Lohrmann described as "a small city." He continued, "It has a library. It has a power generation plant. It has a water plant, a city hall. You can actually hack into them and defend them." Government employees passing the courses are eligible for a variety of certifications.

Michigan Cyber Disruption Response Strategy

According to Mr. Lohrmann, Governor Snyder is a great champion of cybersecurity. "He's really emphasized that cyber disruption is the greatest threat America currently faces .... Nuclear might be number one, but he says the most likely threat is cyber, because it's already happening."

In an effort to create a statewide security strategy, Mr. Lohrmann formed a planning coalition of representatives from key public interests and large employers throughout the state. "We meet monthly, and we have representatives from the top private sector companies in Michigan," explained Mr. Lohrmann. "We've got Consumers Energy, DTE Energy, and some banks. We've also got some auto suppliers and other major businesses in Michigan. We work together to build the cyber-response strategy around how to share information about cyber threats. How do we work together in an emergency? How do we declare an emergency? Who are you going to call? How are we going to coordinate?"

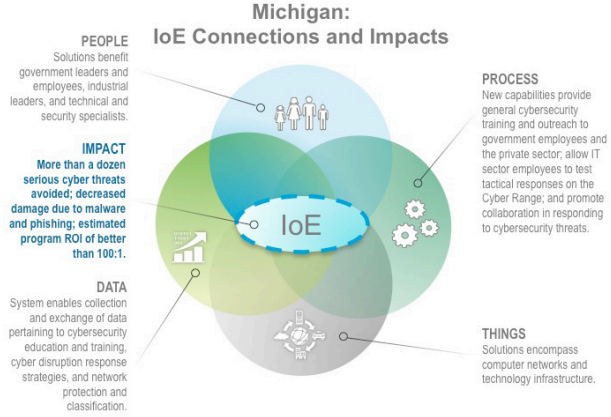
In an effort to create a statewide security strategy, Mr. Lohrmann formed a planning coalition of representatives from key public interests and large employers throughout the state.

The group publishes its conclusions online, in the Michigan Cyber Disruption Response Strategy, which has been named a National Best Practice by the Department of Homeland Security.

"This isn't just outreach and training," Mr. Lohrmann said. "The concept behind this is pretty new. State governments, historically, respond to fires, floods, tornadoes, emergencies. Now we've got potential cyber emergencies. Our Cyber Disruption Strategy was born out of a desire to prepare for a cyber disruption of statewide significance. What if the grid went down? How do we communicate before, during, and after an event? How do we work together with the private sector?" The strategy also includes policies on sharing cyber threat information, how to define an emergency, and a list of emergency contacts.

Mr. Ozols noted, "We're one of the first states to also look at industrial employment or economic development opportunities tied in with cybersecurity. We've spoken to a number of potential partners, including Canada, Israel, and so forth. This is also part of the outreach. It's part of the fact that we have more than a departmental life perspective – we have a statewide perspective."

Figure 1. State of Michigan: New and Better Connections.



Source: Cisco Consulting Services, 2014

Impact

Michigan's cybersecurity initiatives garnered the state an "A" grade in the 2012 Center for Digital Government's Digital States Awards, one of only two states so honored. According to the award's website, Michigan "demonstrated results across all survey categories, and nimble leaders use modernization to implement strategic priorities and operational efficiencies. [These] states show evidence of meaningful collaboration; their performance measures and metrics are widely adopted; and their budget cuts tend to be made strategically."

Michigan's training efforts were also selected by NASCIO in 2013 as the top cybersecurity project among the 50 states. The details of this award can be found at www.nascio.org/awards.

Mr. Ozols pointed out that according to the NASCIO award document, "more than a dozen serious cyber threats have been avoided directly from efforts" related to the program.

The Cyber Range has been widely accepted as an advanced arena for training security professionals, and the National Guard uses the website for its own cyber training.

Michigan's data security measures serve as a model for other states to follow. Mr. Lohrmann explained the impact of the Cyber Disruption Response Strategy document on the national security community, saying it was designated a National Best Practice by the Department of Homeland Security. "This cyber framework is being used as an example of what states should be doing to coordinate with the private sector around critical infrastructure and cybersecurity," Mr. Lohrmann said.

Better trained employees and residents – and correspondingly reduced security risks – are the most prominent benefits of Michigan's cybersecurity training initiatives. Mr. Ozols pointed out that according to the NASCIO award document, "more than a dozen serious cyber threats have been avoided directly from efforts" related to the program. Damage due to malware and phishing scams have decreased, and, given the high costs of serious security breaches, Michigan officials estimate the ROI for the program at "more than 100-to-1."

In addition to training programs, the initiatives also include strengthened security in the form of improved IT infrastructure, including cabling, data networks, wireless, and mobile computing projects.

The initiatives also provide a training venue for nonpublic employees and non-Michigan residents as well, and the state website contains updated information available to anyone with online access. The Cyber Range program provides a venue for both state and national training in data security measures. In addition, Mr. Lohrmann's monthly meetings with industry executives and representatives of public infrastructure create a holistic approach to security that is being copied on the national level.

The programs also create opportunities for ongoing education and security. Outreach at local schools and the creation of cybersecurity initiatives in collaboration with Michigan universities provide an incentive for students to pursue skills and employment in data security fields. As Mr. Lohrmann noted, "Jobs and economic development could be a positive side of cybersecurity."

Lessons Learned / Next Steps

Mr. Lohrmann explained that obtaining quantifiable benefits is always a challenge in measuring the benefits of security programs. “As far as our training, the hard part of this is you don’t know what you don’t know,” he said. “It’s like, ‘How many attacks did we stop? How many people didn’t do something they shouldn’t have done because they had the training?’ It’s hard.”

He continued, “We measure how many will take the training, what their reaction to it is. We ask them if their behavior changed. We do some testing around whether people click on links, for example. The problem with measuring success is that I could be doing really well in running these programs, but it doesn’t necessarily mean I’m going to influence the number of attacks against us. There’s no simple measure of security.”

“Most of all, when we think about data, we think about how people interact with the data, the processes we have around that data, and the technology we use to protect the data. From a cybersecurity perspective, people are a big part of that, and that’s why we do such much around training.”

Dan Lohrmann,

Chief Security Officer, Chief Information Security Officer, and Deputy Director of Cybersecurity and Infrastructure Protection,

Michigan Department of Technology, Management and Budget

Mr. Lohrmann acknowledged that today’s IT environment encourages the collection of vast amounts of data. He advised those seeking to create similar programs to remember that “not all data can be treated the same. You’ve got different types of data. There are lots of non-sensitive data and there are sensitive data. Know what data you have. Get a good handle on what data is important, how you’re protecting it, and how you can share the data. Have an inventory, know what it is, know where it is and what the purposes of it are. How long are you keeping it? How long are you storing it? Is it backed up? All of those types of things are essential.”

Identifying useful data and properly using it is a focus Mr. Lohrmann is attempting to refine. “We have a wider project on how we can share data better to get results and uncover fraud in government or uncover programs to better meet citizen needs, to connect the dots on providing better services to the people that most need help.”

Mr. Lohrmann also described the importance of encrypting sensitive data, “both at rest and in transit.” He said, “That’s a policy that took us a little while to implement, and we’re over 95 percent of the way there. We’re not 100 percent, but we’re doing much better than we were.”

Mr. Lohrmann concluded, “Most of all, when we think about data, we think about how people interact with the data, the processes we have around that data, and the technology that we use to protect the data. From a cybersecurity perspective, people are a big part of that, and that’s why we do so much around training. I’m not going to ever say that we’re going to be perfect, but we have to have people, process, and technology around that data, and we need to make sure we’re thinking long and hard about how we’re protecting citizen data.”

More Information

For more information, please visit http://www.michigan.gov/cybersecurity

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**